REMARKS

The Applicant has amended the claims to clarify that which the Applicant considers to be the invention. The Applicant respectfully submits that amendments to the claim set is fully supported by the originally filed specification.

Claim 6 has been amended to render claim 6 an independent claim to a system. Dependent claims 7-12 are unchanged and depend from independent system claim 6. Protocol method claims 1-5 are unchanged. It is respectfully submitted that this amendment addresses the objection under 37 CFR 1.75(c). Claim 6 has also been amended for clarity and imports certain features from original claim 1. Amended claim 6 is fully supported by reference to original claim 1 and original claim 6, and furthermore by reference to Fig. 3 and the associated description in the specification beginning at page 36.

In relation to the double patenting rejection a terminal disclaimer is filed in compliance with 37 CFR 1.321(c).

At pages 4-6 of the Office Action, the Examiner rejects claims 1-4, 6, 7, 11 and 12 under 35 USC 102(b) as being anticipated by Abraham *et al.* (US 4,799,061). A claim is only anticipated if all of its limitations are present in a single reference in the prior art. Because of the limitations of the claims of the present invention are not present in a Abraham *et al.*, as discussed below, the present invention is not anticipated by Abraham *et al.* and the rejection is traversed. Reconsideration and withdrawal of the rejection is respectfully requested.

Abraham *et al.* discloses a method and system for authenticating hardware or components in a communication system. Abraham *et al.* discloses the requirement that a random number encrypted under the key of one terminal is passed to a second terminal. The second terminal then decrypts the encrypted number using its key, generating the random number, if the keys are identical. The second terminal then encrypts its key using its derivation of the random number, creating its response to the first terminal (col. 2, lines 5-11). It is respectfully submitted that this method is not the method defined in present claim 1 or the system defined in present claim 6 of the subject application. Th present invention is

directed to a double chip validation protocol and system, each chip applying a one-way function to the generated random number based on a secret key.

The Examiner relies on various disclosures in col. 3 of Abraham *et al.* to anticipate the presently claimed invention. However, it is respectfully submitted that there is little material overlap between Abraham *et al.* and the presently claimed invention, as defined in either claim 1 or claim 6, other than encryption and decryption of a random number in separate devices. In Abraham *et al.*, the calculated value B is compared with the value Z from the block 36, on line 37A at block 39A. If the values Z and B are equal (indicating that the keys K1 and K2 are equal), the card or other terminal is identified through line 40A (col. 3, lines 40-44).

This is not the method or system claimed in the present application. Referring to claim 1 of the present application, with reference to the preferred embodiment illustrated in Fig. 3, a random number R is generated from trusted authentication chip 23 and transmitted 31 to system 21. System 21 then requests 32 and 33 application of a one-way function S[R] to random number R (generated from trusted chip 23) in both trusted chip 23 and untrusted chip 20 (chip A). Untrusted chip 20 returns 35 S_{KA} [R]. Trusted chip 23 returns 34 S_{KT} [R] to system 21. System 21 compares S_{KA} [R] with S_{KT} [R] to check the authenticity of untrusted chip 20. Importantly, this is a comparison at system 21 from one-way functions applied at chips (trusted chip 23 and untrusted chip 20). Abraham *et al.* does not disclose application of a one-way function at both a trusted chip and an untrusted chip, the outcomes of which are compared. Abraham *et al.* compares random numbers prior to encryption and subsequent to decryption to check if secret keys K1 and K2 are equal (col. 3, lines 23-31). This is not the method claimed in the present application.

In the present invention, system 21 does not have to comprehend one-way function messages. System 21 merely checks that the responses from the trusted chip and the untrusted chip are the same. System 21 therefore does not require knowledge of the keys. Only authentication chips contain the secret key. In contrast, in Abraham *et al.*, the processor preforming the comparison of the decrypted random number has knowledge of the stored secret key K1.

The presently claimed invention has still further advantages and differences over the invention disclosed in Abraham *et al.* which discloses a relatively simple validation technique relying on simple encryption/decryption of a random number. The present invention, as defined in claim 1 and claim 6, provides a validation protocol and system that is novel and inventive over Abraham *et al.* for its use of comparing the outcomes produced in both the trusted and untrusted chips that have applied a keyed one-way function to a random number, where it is not the random number itself that acts as the validation comparison means. This offers a distinct advantage, as previously mentioned, that the comparison means, for example system 21, does not need knowledge of secret keys for validation.

Nowhere is such a method or system disclosed, taught or suggested in Abraham *et al.*, or in Thomlinson *et al.* (US 5,778,069). Thomlinson *et al.* relates to a pseudo random number generator and merely provides a means of generating a random number. These documents, or any of the other prior art document of records, either taken individually or in combination, do not anticipate or render obvious present claim 1 or 6. The person of ordinary skill in the art is not taught or directed to modify the invention in Abraham *et al.* to make a comparison of the outcomes of applying one-way functions to a random number to compare separate trusted and untrusted chips.

For at least the aforementioned reasons, it is respectfully submitted that independent claims 1 and 6 of the present application are not anticipated by or obvious in light of Abraham *et al.*, or other prior art documents of record. Likewise, the dependent claims of the present application are respectfully submitted to patentable over Abraham *et al.* or Thomlinson *et al.* when taken individually or in combination with any of the other prior art documents of record.

CONCLUSION

In view of the foregoing, it is respectfully requested that the Examiner reconsider and withdraw the rejections under 35 USC 102(b) and 35 USC 103(a). The present application is believed to be in condition for allowance. Accordingly, the Applicant respectfully requests a Notice of Allowance of all the claims presently under examination.

Very respectfully,

Applicant:

SIMON ROBERT WALMSLEY

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: Kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9818 6711